

WHAT IS CLAIMED IS:

1 1. A method for implementing a security risk assessment for a merchant
2 entity having connectivity to a shared network, the method comprising:

3 receiving, from each of a plurality of payment-processing organizations, a set
4 of security requirements defining protocols for implementing commercial transactions over
5 the shared network using instruments identified with the payment-processing organization;

6 developing a security test scheme having a set of test requirements whose
7 satisfaction by the merchant entity is sufficient to ensure compliance with the sets of security
8 requirements defined by each of the plurality of payment-processing organizations; and

9 performing a remote scan of a network site maintained by the merchant entity
10 on the shared network in support of shared-network commercial transactions with a security
11 compliance authority server, the remote scan implementing at least a subset of the set of test
12 requirements to evaluate compliance by the merchant entity.

1 2. The method recited in claim 1 further comprising transmitting a
2 questionnaire to the merchant entity with the security compliance authority server, the
3 questionnaire including queries whose truthful response identifies a level of compliance with
4 at least some of the test requirements.

1 3. The method recited in claim 1 further comprising scheduling an on-site
2 audit at the merchant entity with the security compliance authority server, the on-site audit
3 being structured to follow a prescribed methodology for identifying a level of compliance
4 with at least some of the test requirements.

1 4. The method recited in claim 1 wherein a satisfaction level of the test
2 requirements required for compliance with the test requirements is dependent on a
3 characteristic of the merchant entity.

1 5. The method recited in claim 4 wherein the characteristic comprises a
2 shared-network transaction volume processed by the merchant entity over the shared
3 network.

1 6. The method recited in claim 1 wherein a frequency of performing the
2 remote scan is dependent on a characteristic of the merchant entity.

1 7. The method recited in claim 6 wherein the characteristic comprises a
2 shared-network transaction volume processed by the merchant entity over the shared
3 network.

1 8. The method recited in claim 1 further comprising receiving
2 information describing characteristics of the merchant entity from the merchant entity to limit
3 parameters of the remote scan.

1 9. The method recited in claim 1 further comprising generating a report
2 summarizing a level of compliance by the merchant entity with the set of test requirements as
3 determined from performing the remote scan.

1 10. The method recited in claim 1 wherein the merchant entity comprises
2 an Internet merchant.

1 11. The method recited in claim 1 wherein the merchant entity comprises
2 an Internet merchant gateway.

1 12. A method for assessing a security risk for a merchant entity having
2 connectivity to a shared network, the method comprising:
3 receiving information describing characteristics of the merchant entity from
4 the merchant entity;
5 determining which test requirements of a security test scheme to use in
6 assessing the security risk for the merchant entity, wherein the security test scheme includes a
7 set of test requirements whose satisfaction by the merchant entity is sufficient to ensure
8 compliance with a plurality of sets of security requirements defined by a plurality of
9 payment-processing organizations; and
10 executing the security test scheme with a security compliance authority server
11 in accordance with the determined test requirements.

1 13. The method recited in claim 12 wherein executing the security test
2 scheme comprises performing a remote scan of a network site maintained by the merchant
3 entity on the shared network in support of shared-network commercial transactions with the
4 security compliance authority server.

1 14. The method recited in claim 12 wherein executing the security test
2 scheme comprises scheduling an on-site audit at the merchant entity with the security
3 compliance authority server, the on-site audit being structured to follow a prescribed
4 methodology for identifying a level of compliance with at least some of the test requirements.

1 15. The method recited in claim 12 wherein executing the security test
2 scheme comprises transmitting a questionnaire to the merchant entity with the security
3 compliance authority server, the questionnaire including queries whose truthful response
4 identifies a level of compliance with at least some of the test requirements.

1 16. The method recited in claim 12 wherein determining which test
2 requirements of the security test scheme to use in assessing the security risk for the merchant
3 entity is dependent on a characteristic of the merchant entity.

1 17. The method recited in claim 16 wherein the characteristic comprises a
2 shared-network transaction volume processed by the merchant entity over the shared
3 network.

1 18. The method recited in claim 12 further comprising generating a report
2 summarizing a level of compliance by the merchant entity with the set of determined test
3 requirements as evaluated from executing the security test scheme.

1 19. The method recited in claim 12 wherein the merchant entity comprises
2 an Internet merchant.

1 20. The method recited in claim 12 wherein the merchant entity comprises
2 an Internet merchant gateway.

1 21. A computer-readable storage medium having a computer-readable
2 program embodied therein for direction operation of a security compliance authority server
3 including a communications system, a processor, and a storage device, wherein the computer-
4 readable program includes instructions for operating the security compliance authority server
5 to assess a security risk for a merchant entity having connectivity to a shared network in
6 accordance with the following:

7 receiving, with the communications system, information describing
8 characteristics of the merchant entity;

9 determining, with the processor, which test requirements of a security test
10 scheme to use in assessing the security risk for the merchant entity, wherein the security test
11 scheme is stored on the storage device and includes a set of test requirements whose
12 satisfaction by the merchant entity is sufficient to ensure compliance with a plurality of sets
13 of security requirements defined by a plurality of payment-processing organizations; and
14 executing, with the processor, the security test scheme in accordance with the
15 determined test requirements.

1 22. The computer-readable storage medium recited in claim 21 wherein
2 the instructions for executing the security test scheme comprise instructions for performing a
3 remote scan of a network site maintained by the merchant entity on the shared network in
4 support of shared-network commercial transactions.

1 23. The computer-readable storage medium recited in claim 21 wherein
2 the instructions for executing the security test scheme comprise instructions for scheduling an
3 on-site audit at the merchant entity.

1 24. The computer-readable storage medium recited in claim 21 wherein
2 the instructions for executing the security test scheme comprise instructions for transmitting a
3 questionnaire to the merchant entity.